UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/079,004	02/20/2002	Richard P. Mangold	42390P13346	6126

8791 7590 03/15/2007
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/079,004	**Applicant(s)** MANGOLD ET AL.	
	Examiner Longbit Chai	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 20 February 2002.

2a)□ This action is **FINAL**.   2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-24 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-24 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 20 February 2002 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

The effective filing date for the subject matter defined in the pending claims in this application is 2/20/2002.

Claim Objections

2. Claim 11 is objected to because of the following informalities: "decrypts the content the data content" should be "decrypts the data content". Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 18 – 24 are rejected under 35 U.S.C. 101 because the Claimed invention is directed to non-statutory subject matter. Independent claim 18 is claiming an article of manufacture including computer readable medium and Examiner notes a broad interpretation is reasonably made that a transmission medium can be considered as one type of computer <u>readable</u> media and that, as described in the specification (SPEC: Page 9, Para [0023], Line 1 –2), a transmission medium may be one of many mediums such as satellite transmission. Therefore, the claim limitation is not limited to one of the four

statutory classes on an invention. Examiner respectfully suggested amending the claim language from "one or more computer readable media" to "one or more computer readable storage media" to resolve this pending issue. Any other claims not addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 6 – 8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 6 is indefinite because the claim language "a second security module" has insufficient antecedent basis for this limitation in the claim in lack of a first security module being recited in any of the precedent claims 1 and 5. Any other claims not addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant

> for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 2, 4, 9, 11 – 16, 18 – 19 and 21 are rejected under 35 U.S.C. 102(e) by Aleksic et al. (U.S. Patent 6,957,329).

As per claim 1 and 18, Aleksic teaches a method comprising:

receiving video data at an application program (Aleksic: Column 1 Line 33 – 38);

storing a first list of hardware registers (Aleksic: Column 8 Line 47 – 51, Column 3 Line 42 – 48 and Figure 1 / Element 143 – 146: the encryption seed key values are stored in hardware registers that can be used for content decryption at the encryption / decryption engine);

receiving a second list of hardware registers from a device driver (Aleksic: Column 4 Line 33 – 38, Column 6 Line 56 – 62 and Column 5 Line 11 – 13: the authentication engine at the driver interfacing / synchronizing between the hardware ciphering engine and applications by providing the available keys to the applications and the available keys are depending upon the available hardware registers);

determining whether the first list of hardware registers matches the second list of hardware registers; and if so, streaming the video data to a video decoder (Aleksic: Column 5 Line 11 – 13 and Column 5 Line 3 – 5 / Line 49 – 52 / Line 22 – 48: during the transition period of using the old / new keys, in re-authentication process due to data error, the driver can wait until all the encrypted data, based on the old key value, is all sent and the buffer is clear before using the new key value to process the digital data – i.e. the driver is holding the encrypted data from the applications in the buffers before sending to the hardware ciphering engine until the tracking assures that both multimedia application and hardware section use the same new / old key value registers).

As per claim 9, Aleksic teaches a computer system comprising:

a player application that receives data content (Aleksic: Column 2 Line 48 – 49 and Figure 1);

a decoder that stores and decodes the data content received at the player, the decoder including hardware registers to store the data content (Aleksic: Column 8 Line 47 – 51, Column 3 Line 42 – 48 and Figure 1 / Element 143 – 146: the encryption seed key values are stored in hardware registers that can be used for content decryption at the encryption / decryption engine);

a driver, coupled to the decoder that allocates the hardware registers within for access by the player application (Aleksic: Column 4 Line 33 – 38, Column 5 Line 11 – 13 and Figure 1 / Element 130: the authentication engine at the driver interfacing / synchronizing between the hardware ciphering engine and applications by providing the available keys to the applications and the available keys are depending upon the available hardware registers);

a first security module, coupled to the driver, that secures a first list of resources corresponding to the hardware registers to prevent unauthorized access of the data content within the hardware registers (Aleksic: Column 5 Line

11 – 13 and Column 5 Line 3 – 5 / Line 49 – 52 / Line 22 – 48: (a) the authentication engine, considered as a first security module, at the driver interfacing / synchronizing between the hardware ciphering engine and applications by providing the available keys to the applications and the available keys are depending upon the available hardware registers (b) during the transition period of using the old / new keys, in re-authentication process due to data error, the driver can wait until all the encrypted data, based on the old key value, is all sent and the buffer is clear before using the new key value to process the digital data – i.e. the driver is holding the encrypted data from the applications in the buffers before sending to the hardware ciphering engine until the tracking assures that both multimedia application and hardware section use the same new / old key value registers).

As per claim 2 and 19, Aleksic teaches precluding the streaming of the video data to the video decoder if the first list of hardware registers does not match the second list of hardware registers (Aleksic: Column 5 Line 11 – 13 and Column 5 Line 3 – 5 / Line 49 – 52 / Line 22 – 48: the driver is holding the encrypted data from the applications in the buffers before sending to the hardware ciphering engine until the tracking assures that both multimedia application and hardware section use the same new / old key value registers).

As per claim 4 and 21, Aleksic teaches encrypting the first list of hardware registers prior to storing the first list of hardware registers (Aleksic: Column 4

Line 25 – 32: a simple MATH function, such as sum / add, is used equivalently for encrypting purpose).

As per claim 11, Aleksic teaches an interface, coupled to the player application, the driver and the decoder, that decrypts the content the data content prior to the data content being stored in the hardware registers (Aleksic: Column 4 Line 34 – 38, Column 9 Line 62 – 64, Column 4 Line 18 – 21 and Column 8 Line 47 – 51: the data content is decrypted first and the generated content is combined with the final / last key values to create the new key values that are then stored in the hardware key registers for later use).

As per claim 12, Aleksic teaches the driver verifies the integrity of the interface via digital signatures and public/private key technologies (Aleksic: Column 8 Line 6 – 8 and Column 14 Line 40 – 46).

As per claim 13, Aleksic teaches a second security module coupled to the interface and the first security module (Aleksic: Column 6 Line 56 – 63 and Column 5 Line 11 – 13: (a) the <u>second</u> security module is interpreted as the authentication security entity interfacing between the application and the driver that negotiates about a list of available encryption keys on the multimedia application requesting the authentication and (b) a <u>first</u> security module is interpreted as the authentication engine at the driver interfacing / synchronizing between the hardware ciphering engine and applications by providing the available keys to the applications and the available keys are depending upon the available hardware registers).

As per claim 14, Aleksic teaches the second security module receives a second list of resources from the interface whenever the player application is to release the data content from the hardware registers (Aleksic: Column 6 Line 56 – 63: the authentication security entity interfacing between the application and the driver that negotiates about a list of available encryption keys on the multimedia application requesting the authentication upon decrypting the digital content).

As per claim 15, Aleksic teaches the second security module retrieves the first list of resources from the first security module and compares the first list of resources to the second list of resources (Aleksic: Column 6 Line 56 – 63 and Column 5 Line 3 – 5 / Line 49 – 52 / Line 22 – 48: during the transition period of using the old / new keys, in re-authentication process due to data error, the driver interface to application side (or the second security module) holding the encrypted data from the applications in the buffers before sending to the hardware ciphering engine until the tracking assures that both multimedia application and hardware section use the same new / old key value registers).

As per claim 16, Aleksic teaches the data content is released from the hardware registers if the second list of resources matches the first list of resources (Aleksic: Column 6 Line 56 – 63 and Column 5 Line 49 – 52: holding the encrypted data from the applications in the buffers before sending to the hardware decoding engine until the tracking of the key registers used by both hardware section and applications match, for example, both use new key value, during the transition period of using the old / new keys, in re-authentication process due to data error, the driver interface to application side (or the second security module)).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 3, 10 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aleksic et al. (U.S. Patent 2002/0144153), in view of Zimmer (U.S. Patent 6,978,018).

As per claim 3 and 20, Aleksic teaches initializing the device driver upon startup of a computer system (Examiner notes: each device driver must be first initialized upon startup of a computer system) forwarding the first list of hardware registers from the device driver to a first security module (Aleksic: Column 3 Line

51 – 59 and Column 5 Line 11 – 13: the authentication engine, considered as a first security module, at the driver interfacing / synchronizing between the hardware ciphering engine and applications and is informed about which available hardware key registers to be used);

Aleksic does not disclose expressly verifying, at the first security module, a digital signature of the device driver prior to storing the first list of hardware registers.

Zimmer teaches verifying, at the first security module, a digital signature of the device driver prior to storing the first list of hardware registers (Zimmer: Column 14 Line 40 – 46: verifying an integrity of the runtime driver using a digital signature key to determine whether the runtime driver file has been altered from an original form).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Zimmer within the system of Aleksic because (a) Aleksic teaches the driver interfacing / synchronizing between the hardware ciphering engine and applications when providing the available keys to the applications and the hardware ciphering engine (Aleksic Column 5 Line 11 – 13 and Column 5 Line 3 – 5 / Line 22 – 52) and (b) Zimmer teaches providing enhanced security mechanism by verifying an integrity of the runtime driver using a digital signature key to determine whether the runtime driver file has been altered from an original form (Zimmer: Column 14 Line 40 – 46).

As per claim 10, Aleksic teaches the first security module (Aleksic: Column 3 Line 51 – 59 and Column 5 Line 11 – 13: the authentication engine, considered as a first security module, at the driver interfacing / synchronizing between the hardware ciphering engine and applications by providing the available keys to the applications and the available keys are depending upon the available hardware registers). However, Aleksic does not disclose expressly the first security module verifies the integrity of the driver via digital signatures prior to receiving the first list of resources.

Zimmer teaches the first security module verifies the integrity of the driver via digital signatures prior to receiving the first list of resources (Zimmer: Column 14 Line 40 – 46: verifying an integrity of the runtime driver using a digital signature key to determine whether the runtime driver file has been altered from an original form). See same rationale of combination applied herein as above in rejecting the claim 3.

7. Claims 5 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aleksic et al. (U.S. Patent 2002/0144153), in view of Wyland (U.S. Patent 2003/0065863).

As per claim 5 and 22, Aleksic teaches the application program calling an interface upon receiving the video data (Aleksic: Column 6 Line 43 – 46: driver interfaces between the application and the hardware section); the interface requesting the second list of hardware registers from the device driver (Aleksic:

Column 6 Line 47 – 48 / Line 58 – 64: authentication request from applications to the driver for a list of available encryption keys).

However, Aleksic does not disclose expressly mapping the second list of hardware registers to a virtual resource map that is accessible by the application.

Wyland teaches mapping the second list of hardware registers to a virtual resource map that is accessible by the application (Wyland: Para [0029] / Page 3 Line 28 – 30: a virtual hardware register is used and accessed by the application layer through virtual I/O devices which are mapped into the system address space to enable the application access. This is also commonly used in software engineering as a well known "memory-map-I/O").

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Wyland within the system of Aleksic because (a) Aleksic teaches the driver interfacing / synchronizing between the hardware ciphering engine and applications by providing the available keys to the applications and the available keys are depending upon the available hardware registers (Aleksic Column 5 Line 11 – 13 and Column 5 Line 3 – 5 / Line 22 – 52) and (b) Wyland discloses an effective and well-known "memory-map-I/O" mechanism, where a virtual hardware register is used and accessed by the application layer through virtual I/O devices which are mapped into the system address space to enable the application access).

8. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Aleksic et al. (U.S. Patent 2002/0144153), in view of Farber et al. (U.S. Patent 6,920,221).

As per claim 17, Aleksic does not disclose expressly the connection between the first security module and the second security module is secured by a random number secret key system.

Farber teaches the connection between the first security module and the second security module is secured by a random number secret key system (Farber: Column 3 Line 53 – 56: video hardware interface and video source application are assumed to have each been provided with an array of private "cryptographic" keys that are pre-provided with an array of 56-bit private "cryptographic" keys by the certification authority, where Cn is a 64-bit random number).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Farber within the system of Aleksic because (a) Aleksic teaches the driver interfacing / synchronizing between the hardware ciphering engine and applications on encryption / decryption of digital content (Aleksic Column 5 Line 11 – 13 and Column 5 Line 3 – 5 / Line 22 – 52) and (b) Farber teaches providing a secured data exchange interface between the hardware interface and source application by pre-providing an array of 56-bit private "cryptographic" keys derived from a 64-bit random number (Farber: Column 3 Line 53 – 56).

Allowable Subject Matter

9. Claims 6 – 8 and 23 – 24 are objected to as being dependent upon a rejected base claim but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is an examiner's statement of reasons for allowance: The present invention is directed to a method for digital content copyright protection where the application level interface forwards the virtual memory address to an application level security module to validate the hardware registers to which the application intends to stream the content – as per claim 6 and 23 (& its dependent claims 7 – 8 and 24), the claim limitations recite the interface calling a second security module to verify the second list of hardware registers; and the second security module calling the first security module in order to verify the virtual resource map. The closest prior art, U.S. Pattern 6,957,329 and U.S. Pattern 2003/0065863, fail to anticipate or render obvious the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LongBit Chai

Longbit Chai, Ph.D.
Patent Examiner
Art Unit 2131
2/8/2007